# Writeup-GKCTF-Misc题： Harley Quinn

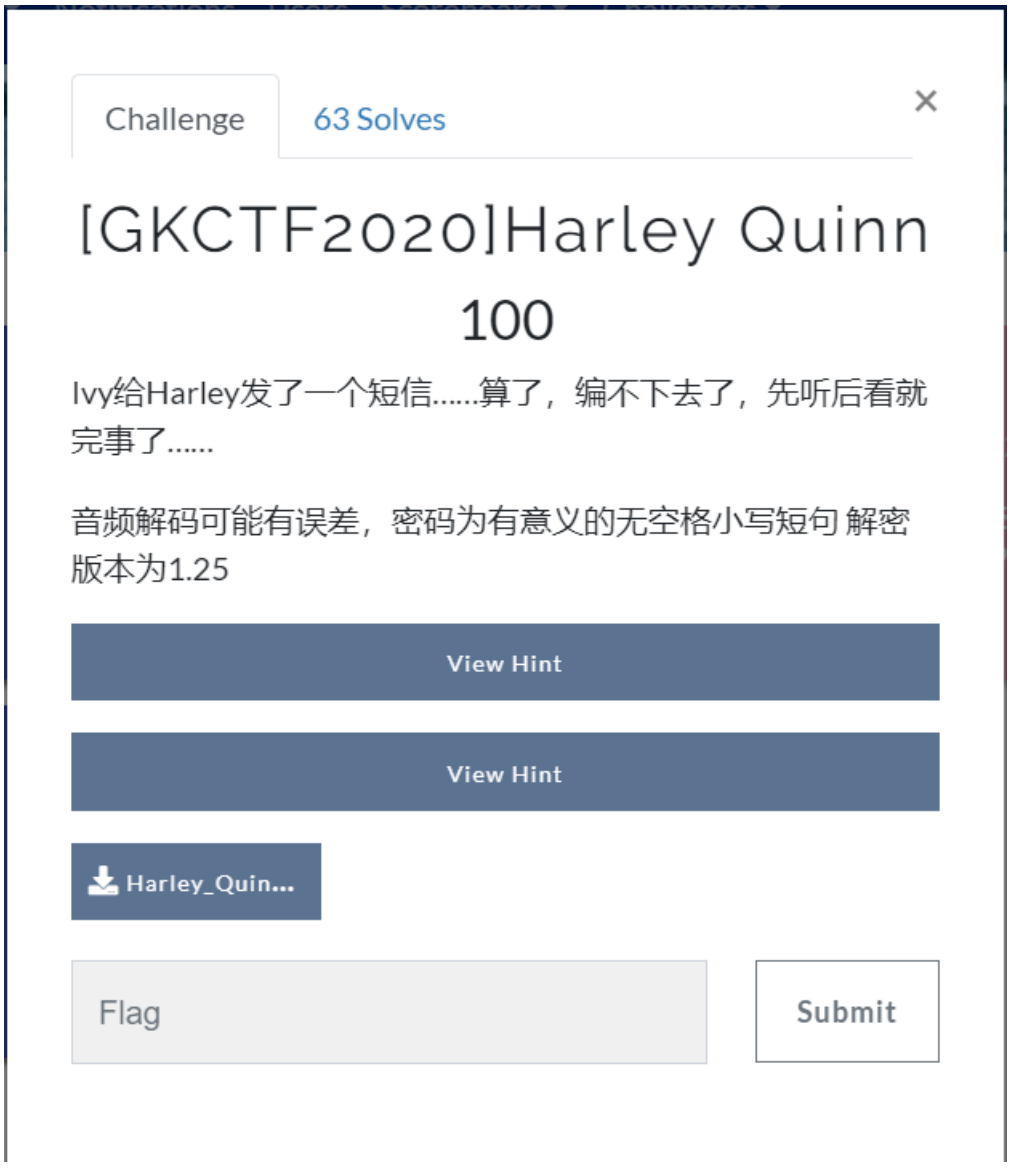
原创

Y5neKO 于 2020-05-29 11:54:50 发布 69 收藏
文章标签： 信息安全 安全 windows linux 百度

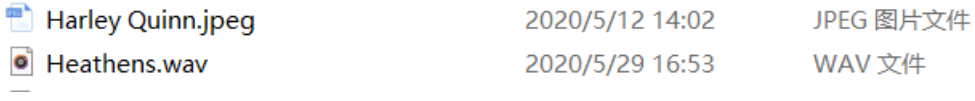
本文链接：https://blog.csdn.net/qq_41596969/article/details/110377832


小丑女！

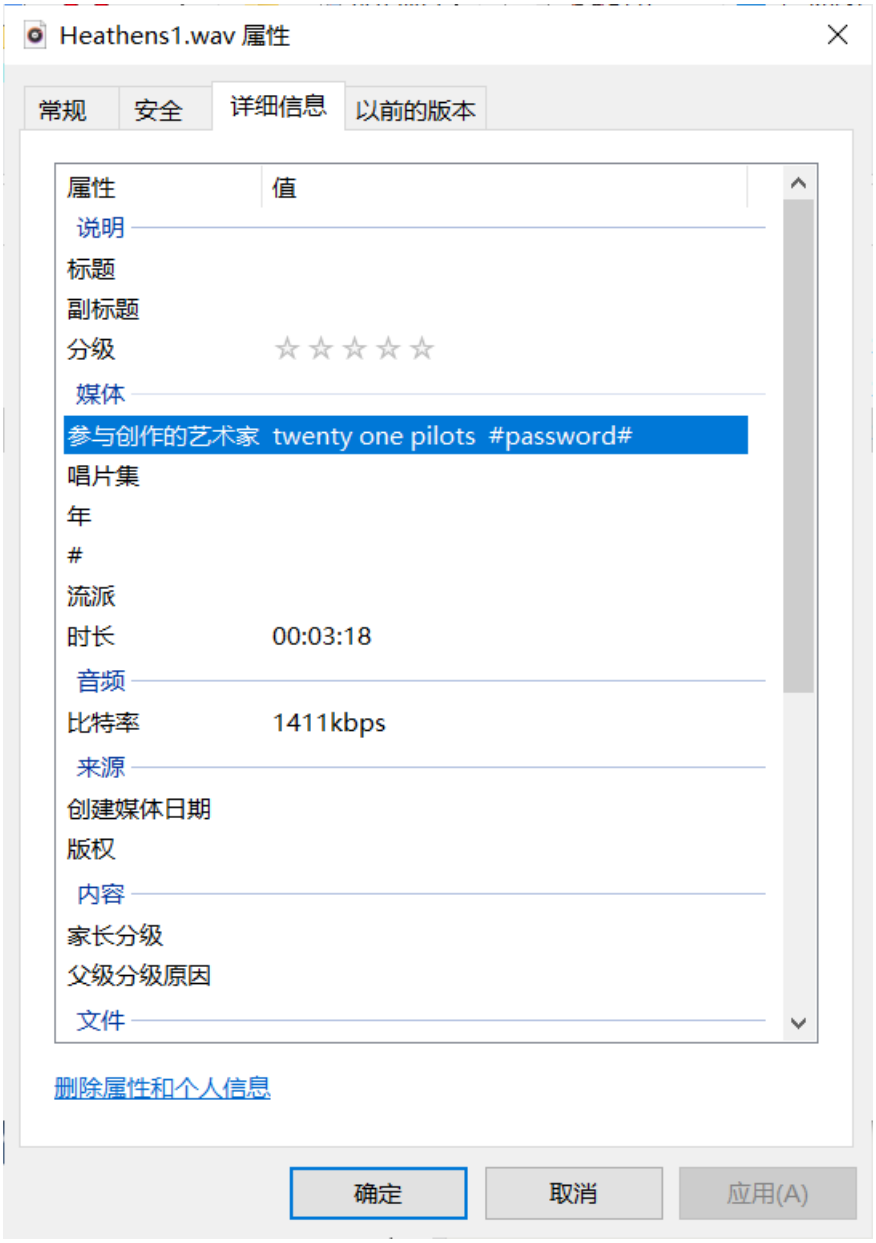
原题地址：https://buuoj.cn/challenges#[GKCTF2020]Harley%20Quinn



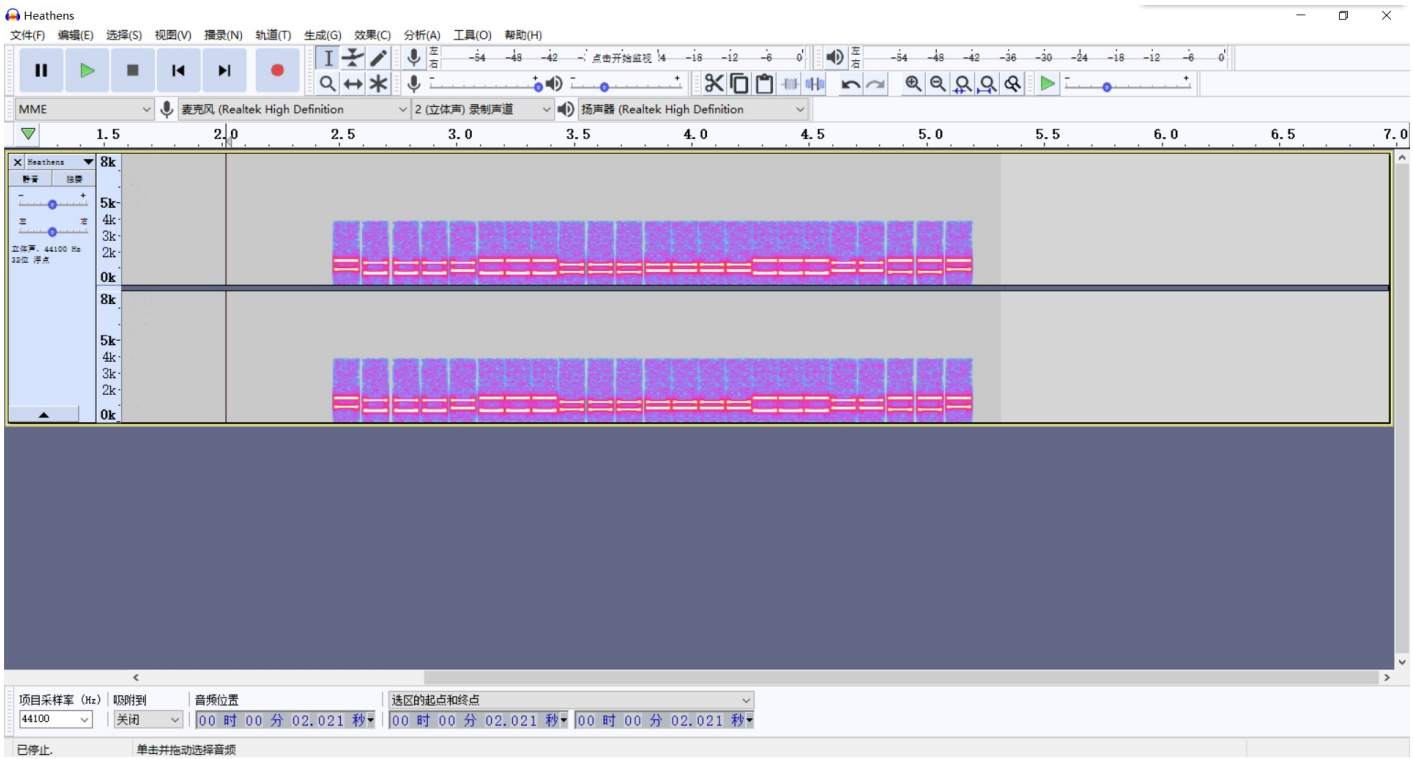

首先读题，这应该是一道音频隐写题
把附件下载下来，里面有一个wav音频和一张jpeg图片



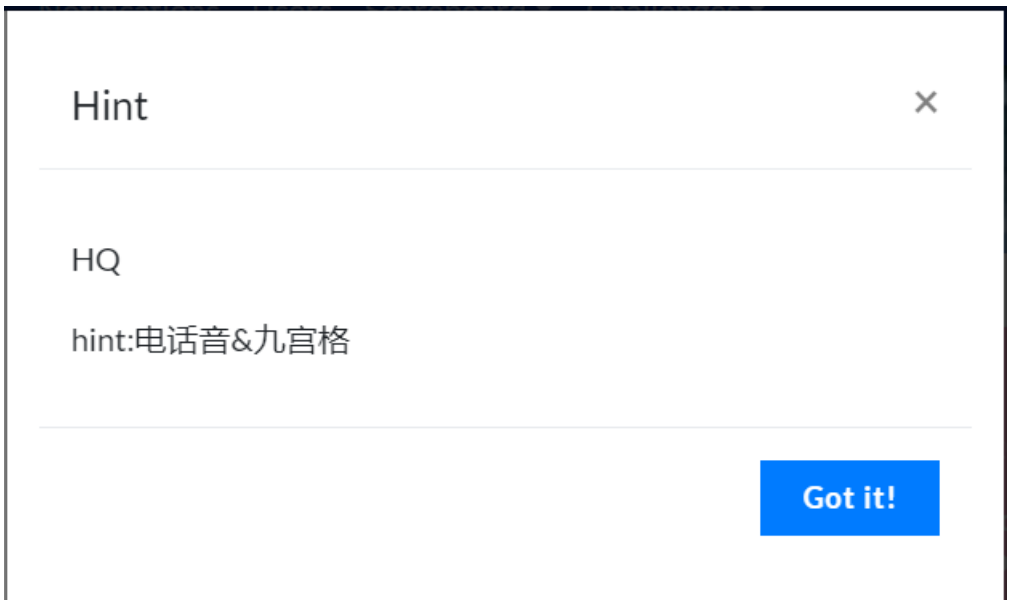

图片暂时还不知道有什么用，我们听一下音频，是twenty one pilots的Heathens
歌不错，可是我寻思着这也没啥线索啊，右键查看歌曲属性，在作曲家信息找到了线索




根据长达几个月的ctf经验来看，音频中应该藏着一段21位的password
开始着手分析，把这段音频导入audocity，打开频谱分析，粗略一看没发现什么，最后在音频末尾发现这样一段




DTMF双音多频，熟悉的按键音频谱，看了一下题目中的hint确实如此




然后到这里就卡住了。。。因为我从来没有搞懂大佬们是如何分析频谱图的，貌似需要matlab建模分析什么的，听的我是一头雾水

这里就要提到一个多年前的神器了，不经意间发现的，叫做`dtmf2num.exe`

现在网上基本找不到下载地址了，我这里给大家一个：https://lanzous.com/id4e4hc

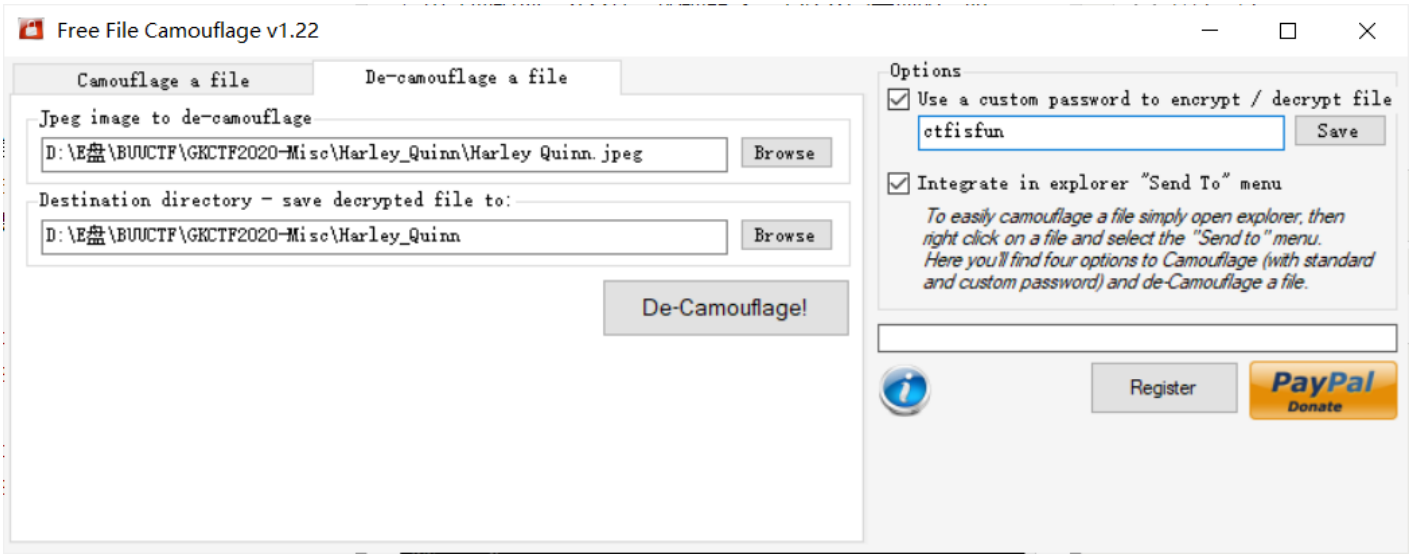
这个神器是个命令行工具，可以直接分析音频的频谱得出按键，但因为是比较老的工具了，嘈杂环境下辨识度很低，好在这次音频是电脑直接合成的，因此可以直接识别

使用之前注意先将前面歌曲部分剪辑掉，因为这个软件只能分析几十秒内的音频，剪辑好后在cmd环境下直接加文件名就可以，分析结果如下

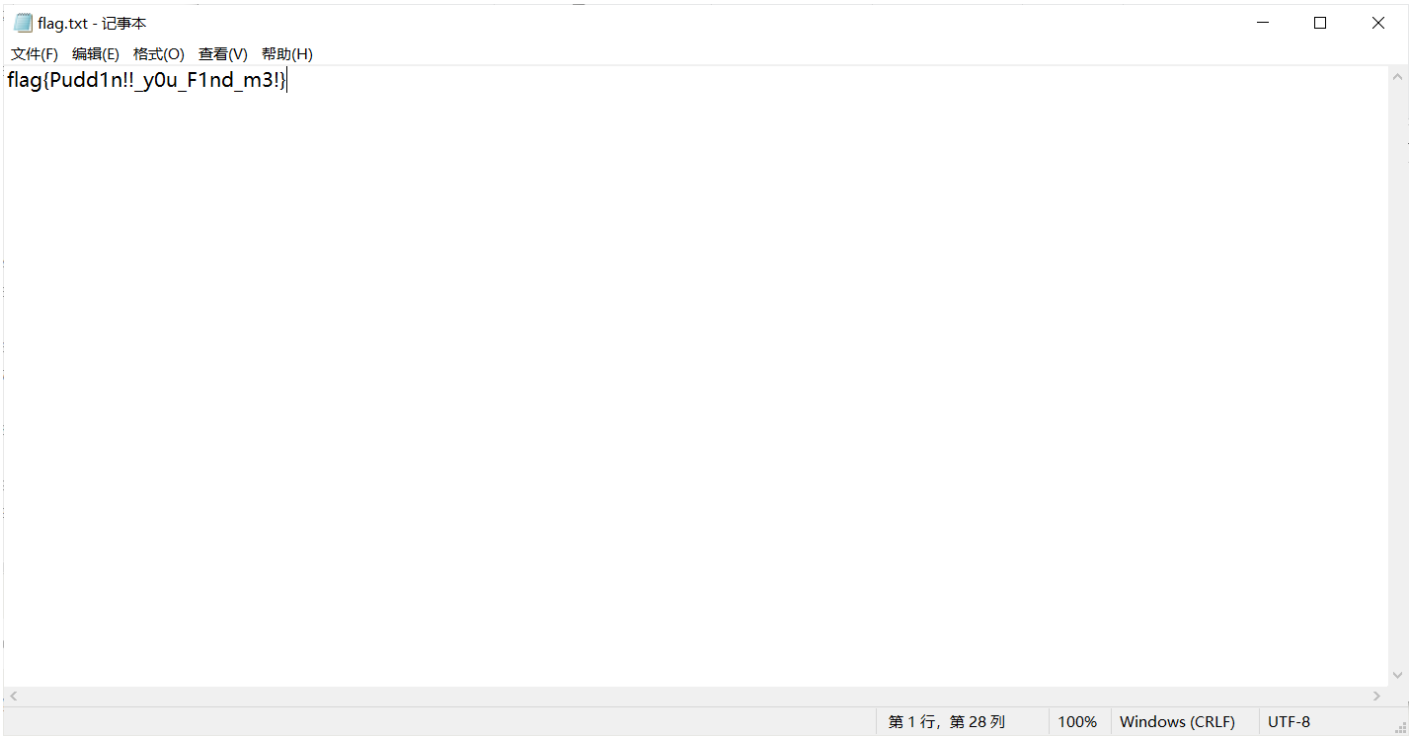
```
管理员: C:\Windows\System32\cmd.exe

D:\音频分析>dtmf2num Heathens.wav

DTMF2NUM 0.1c
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- open Heathens.wav
  wave size      938448
  format tag     1
  channels:      2
  samples/sec:   44100
  avg/bytes/sec: 176400
  block align:   4
  bits:          16
  samples:       469224
  bias adjust:   14
  volume peaks:  -31205 31205
  normalize:     1562
  resampling to: 8000hz

- MF numbers:    44477

- DTMF numbers:  #222833444777733338866#

D:\音频分析>
```

正好与前面提到的信息吻合：twenty one pilots #password#
数了一下发现密码少了一位，对比频谱图发现因为播放速度的原因少分析了一位，结合前后频谱得到正确结果：`#222833344477773338866#`
从hint可以知道这个对应的是九键键盘密码，所以最终得到的密码为：`ctfisfun`


那么拿到密码该到哪里用呢，从第二条hint看：FreeFileCamouflage
百度了一下，这个软件能将文件隐藏在jpg图片中
因此我们将附件里里的小丑女图片用FreeFileCamouflage解密，如图填好，点击De-Camouflage解密




成功得到flag.txt




最终flag为：

```
flag{Pudd1n!!_y0u_F1nd_m3!}
```